Patent Abstract

GER 1994-02-03 4308899 **Procedure for the enterprise of a concluding system remote controlable; in a dialogue procedure, e.g. a Kfz.**
ANNOTATED TITLE- Verfahren zum Betrieb eines in einem Dialogverfahren fernsteuerbaren Schlieo"systemes, z.B. eines Kfz.

INVENTOR- Hiebl, Johann

APPLICANT- Siemens AG
PATENT NUMBER- 04308899/DE-C1
PATENT APPLICATION NUMBER- 04308899
DATE FILED- 1993-03-19
DOCUMENT TYPE- C1, PATENT SPECIFICATION (FIRST PUBL.)
PUBLICATION DATE- 1994-02-03
INTERNATIONAL PATENT CLASS- E05B04900; E05B06512; G07C00900E14C
PATENT APPLICATION PRIORITY- 4308899, A
PRIORITY COUNTRY CODE- DE, Germany, Ged. Rep. of
PRIORITY DATE- 1993-03-19
FILING LANGUAGE- German
LANGUAGE- German NDN- 203-0317-5563-0

Procedure for the enterprise in a dialogue procedure remote; controlable of a concluding system, with a portable key unity and a; lock unity contains, whereby in each case the codes (n, x, y, y+1) of; the signals (1, 2, 3) represent change codes. First a first signal (1); is sent to the conclude-lateral payee, whereby this signal with a; first, actually valid code formed pursuant to a first algorithm is; modulated (n). To it the lock unity, if its computer (E) recognizes; the received first code (n) as valid, sends a second signal (2) to the; key-lateral payee, whereby this signal with a second code is modulated; (x). To it the key unity, if its computer recognizes the received code; (x) as valid, sends a third signal (33) to the lock unity, whereby; this signal with a third code formed pursuant to the first algorithm; is modulated (y). The lock unity steers the lock, if their computer; recognizes the received third code as valid.
EXEMPLARY CLAIMS- 1. Procedure for the enterprise in a dialogue procedure by signals (l, 2, 3), i.e. coded radio -, light-or ultrasonic signals, remote controlable e.g. lockable and unlockable closing system of an object, e.g. a Kfz, with a portable key unit, which contains a key-lateral transmitter, a key-lateral receiver and a key-lateral computer (S), with a lock unit, which contains a close-lateral transmitter, a close-lateral receiver, a close-lateral computer (E) and an output unit for control (V) the lock e.g. for the controlling of the bolting device of the lock , appropriate at the object, whereby the codes (n, x, in each case y, y +1) of the signals (l, 2.3) change code represent, which linked algorithmically, both in the key-lateral and in the close-lateral computer generated code sequences (e.g. code n, code x = n +1, code y = n+2....) represent, and whereby the individual codes, which are formed in the key unit (S) for of them to out-send in each case signals (l, 3), in each case e.g. by the manipulation of the key unit or steered by a clock in accordance with a first algorithm to be incremented, by it characterized, that with manipulation of the key unit its transmitters first a first signal (1) to the close-lateral receiver sends, whereby the first signal (1) with a first, up-to-date valid code (n) from the first algorithm corresponding the code sequence, formed in accordance with the first algorithm, is modulated, that to it the first signal (I) receiving lock unit, if its computer (E) recognizes the received first code (n) as the valid first code (n), for their part as answer a second signal (2) to the key-lateral receiver sends, whereby the second signal (2) with one in accordance with a second algorithm (f (n)) formed second, to up-to-date valid code (x=f (n)) from that the second algorithm (f (n) appropriate code sequence is modulated, that thereafter

the key unit for its part as answer, if its computer (S) the received the code with the second signal (2) (x = f

NO-DESCRIPTORS

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 43 08 899 C 1**

(51) Int. Cl.[5]:
E 05 B 49/00
E 05 B 65/12

(21) Aktenzeichen: P 43 08 899.6-31
(22) Anmeldetag: 19. 3. 93
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 3. 2. 94

DE 43 08 899 C1

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Siemens AG, 80333 München, DE

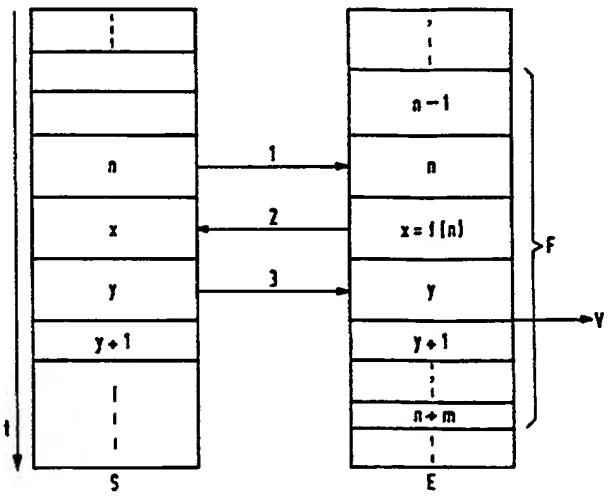
(72) Erfinder:
Hiebl, Johann, Dipl.-Ing. (FH), 8411 Bernhardswald, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE 36 36 822 C1
DE 35 36 378 A1
DE 32 25 754 A1

(54) Verfahren zum Betrieb eines in einem Dialogverfahren fernsteuerbaren Schließsystemes, z.B. eines Kfz

(57) Verfahren zum Betrieb eines in einem Dialogverfahren fernsteuerbaren Schließsystems, mit einer tragbaren Schlüsseleinheit und einer Schloßeinheit enthält, wobei die Codes (n, x, y, y+1) der Signale (1, 2, 3) jeweils Wechselcodes darstellen. Zuerst wird ein erstes Signal (1) zum schloßseitigen Empfänger gesendet, wobei dieses Signal mit einem gemäß einem ersten Algorithmus gebildeten ersten, aktuell gültigen Code (n) moduliert ist. Danach sendet die Schloßeinheit, wenn ihr Rechner (E) den empfangenen ersten Code (n) als gültig erkennt, ein zweites Signal (2) zum schlüsselseitigen Empfänger, wobei dieses Signal mit einem zweiten Code (x) moduliert ist. Danach sendet die Schlüsseleinheit, wenn ihr Rechner den empfangenen Code (x) als gültig erkennt, ein drittes Signal (33) zur Schloßeinheit, wobei dieses Signal mit einem gemäß dem ersten Algorithmus gebildeten dritten Code (y) moduliert ist. Die Schloßeinheit steuert das Schloß, wenn ihr Rechner den empfangenen dritten Code als gültig erkennt.



DE 43 08 899 C1

Beschreibung

Verfahren zum Betrieb eines in einem Dialogverfahren fernsteuerbaren Schließsystemes, z. B. eines Kfz.

Schließsysteme, die mit einem sog. Wechselcode betrieben werden, sind dem einschlägigen Fachmann in sehr vielen Ausführungen bekannt. Grob kann man die Bildung des Wechselcodes dieser bekannten Systeme in zwei Gruppen einteilen:

— in eine erste, bei der die Codes in den Schlüsseleinheiten jeweils durch eine (Quarz-)Uhr modifiziert werden, weswegen diese Schlüsseleinheiten je nach Uhrzeit verschiedene Codes abstrahlen; und
— in eine zweite, bei der die Codes erst unmittelbar durch Betätigen der Schlüsseleinheit, von Betätigung zu Betätigung der Schlüsseleinheit, gemäß einem dafür in der Schlüsseleinheit gespeicherten Algorithmus fortgeschaltet werden.

Die Bildung der Wechselcodes bei der Erfindung gehört bevorzugt zu der zweiten Gruppe von Schließsystemen, weil dort die Probleme der Synchronisation geringer als bei der erster Gruppe ist. Die Erfindung ist aber im Prinzip auch auf die Wechselcodebildung gemäß der ersten Gruppe anwendbar.

Beim laufenden Betrieb dieser zur zweiten Wechselcodebildungsgruppe gehörenden Schließsysteme ist jeder ausgesendete Code jeweils ein spezieller Code aus einer langen folge von Codes. Alle diese Codes der Codefolge werden, ausgehend von einem ursprünglich initialisierenden Urcode, in der Schlüsseleinheit von Betätigung zu Betätigung nach ein und demselben Algorithmus gebildet. Unter diese zweite Gruppe fällt auch ein bekanntes Schließsystem, bei dem das Schloß im Fahrzeug erst nach zweimaliger Betätigung der Schlüsseleinheit gesteuert wird, so daß die Schlüsseleinheit zwei gemäß ihrem Algorithmus aufeinander folgende unterschiedliche Codes ihrer Codefolge aussenden muß, bevor das Schloß gesteuert wird, vgl.

— DE-A1-35 36 378, ab Spalte 4, Zeile 25.

Die Erfindung geht von dem im Oberbegriff des Patentanspruches 1 definierten Gegenstand aus, der für sich, betrieben mit einem Wechselcode gemäß der oben angegebenen zweiten Gruppe, vorbekannt ist, vgl.

— DE-A1-32 25 754, besonders die dortigen Erläuterungen von Tabellen 1 und 2 ab Seite 9, letzter Absatz.

Bei diesem Stande der Technik ist aber der erste ausgesendete Code nicht ein Code aus einer langen Folge von Codes, die alle, ausgehend von einem initialisierden Urcode, in der Schlüsseleinheit nach ein und demselben ersten Algorithmus gebildet werden.

Die Erfindung wurde zwar zunächst für ein Kfz entwickelt. Es zeigte sich aber, daß sie darüber hinaus auch auf andere, unter den genannten Oberbegriff fallende Schließsysteme anwendbar ist. Die Erfindung ist nämlich z. B. auch für Garagen, Lagerhallen, Haustüren usw. geeignet.

Ein Hauptproblem solcher Verfahren ist die Vermeidung von Einbrüchen, die Einbrechern durch ein verbotenes Aufzeichnen von codierten Signalen, die die Originalschlüsseleinheit aussendet, möglich werden. Besonders dann, wenn die Schlüsseleinheit einmal versehentlich aktiviert wurde, ohne daß die Schloßeinheit dieses Signal empfangen konnte, dann könnte normalerweise der Einbrecher bereits durch das Aufzeichnen des Code dieses versehentlich abgestrahlten Signales einbrechen, indem er diesen Code dem Empfänger der Schloßeinheit rechtzeitig zusendet, bevor der Code — warum auch immer — fortgeschaltet ist.

Die Aufgabe,
— dem Einbrecher das Einbrechen besonders stark zu erschweren, wird erfindungsgemäß durch den im Patentanspruch 1 definierten Gegenstand gelöst.

Die in den Unteransprüchen definierten Gegenstände gestatten, zusätzliche Vorteile zu erreichen. U.a. gestatten nämlich die zusätzlichen Maßnahmen gemäß dem Patentanspruch
2. den Einbruch besonders stark zu erschweren, weil der Einbrecher, auch wenn er ein gemäß dem zweiten Algorithmus gebildetes zweites Signal mitabgehört hätte, nur besonders schwer erraten kann, nach welchem Algorithmus das erste und das dritte Signal gebildet wurde, besonders falls das Aufzeichnungsgerät des mithörenden Einbrechers zusätzlich Schwierigkeiten hatte, die drei ausgetauschten verschiedenen Signale deutlich voneinander zu trennen, — besonders wenn bei dieser Variante der Erfindung eine besonders rasche lückenlose — oder sogar sich bewußt überlappende — Aufeinanderfolge der drei Signale eingerichtet wird; überdies schaltet beim erfindungsgemäßen Wechselcode das ganze Schließsystem nach einer ordnungsgemäßen Betätigung des Schließsystemes rasch auf neue Codes der Codefolge/Codefolgen um, bevor der Einbrecher die mitgehörten, aufgezeichneten für den Einbruch unmittelbar benutzen könnte,
3. eine besonders unkomplizierte Möglichkeit zu bieten, die — wegen der Notwendigkeit, daß der Einbrecher z. B. die Codes des ersten und des dritten Signales simulieren müßte — bereits sehr stark gegen einen Einbruch durch Codemanipulationen gesichert ist, weil es für den Einbrecher bereits äußerst schwierig ist, den benutzen ersten Algorithmus ausfindig zu machen,
4. in für sich bekannter Weise den Verlust der Synchronisation der Codes in der Schlüsseleinheit mit den Codes in der Schloßeinheit zumindest in den meisten Fällen durch eine automatische Nachsynchronisation rückgängig zu machen, falls nämlich der Code in der Schlüsseleinheit durch ein versehentliches mehrmaliges Betätigen dieser Schlüsseleinheit versehentlich um viele Schritte fortgeschaltet wurde, ohne daß auch der Code in der Schloßeinheit fortgeschaltet wurde,
5. eine Nachsynchronisation bei versehentlichen Betätigungen der Schlüsseleinheit zumindest i. allg. vermeiden zu können,
6. eine automatische Nachsynchronisation in einem sehr kleinen Fangbereich, der z. B. nur zwei oder drei Fortschaltungen des Codes umfaßt, für den Fall zu ermöglichen, daß zwar der erste und der zweite Code einwandfrei übertragen wurde, daß aber der dritte Code — warum auch immer — nicht mit dem unbedingt nötigen Leistungspegel den schloßseitigen Empfänger erreichte,
7. eine Einstellung des schloßseitigen Rechners auf den nächsten aktuell gültigen Code für ein nächstes erstes Signal nur zuzulassen, wenn der schloßseitige Empfänger zuvor unverzüglich das richtig codierte dritte Signal empfing,
8. besonders stark zu erschweren, durch das Mithören eines Dialoges Rückschlüsse auf den benutzten Algorithmus / die benutzten Algorithmen zu ziehen, und
9. ein Schließsystem zu bieten, das gerade die Vorteile

der in den vorhergehenden Verfahrensansprüchen angegebenen Maßnahmen auszunutzen gestattet.

Die Erfindung und Weiterbildungen derselben werden anhand eines Ausführungsbeispieles der Erfindung, nämlich anhand eines in der Figur gezeigten Schemas für die Fortschaltung der im Dialogverfahren ausgetauschten Codes, weiter erläutert. Diese Figur zeigt das erfindungsgemäße Beispiel bewußt der Übersichtlichkeit wegen in möglichst einfacher Darstellung.

Die Figur zeigt also ein Beispiel für den erfindungsgemäßen Betrieb eines im Dialogverfahren durch die ausgetauschten Signale 1, 2, 3 fernsteuerbaren — z. B. verriegelbaren und entriegelbaren — Schließsystemes eines Kfz. Angenommen sei, daß die Codebildung gemäß der oben beschriebenen zweiten Gruppe erfolgt, daß also der Code der Schlüsseleinheit von deren Betätigung zu deren nächsten Betätigung fortgeschaltet werden kann, — zumindest solange diese Schlüsseleinheit jeweils ein aktuell gültig moduliertes zweites Signal 2 vom Sender der Schloßeinheit empfängt. E symbolisiert in der Figur den Betrieb des schloßseitigen Rechners und S den Betrieb des schlüsselseitigen Rechners, jeweils im Verlauf der — auch bei dieser Art von Wechselcodebildung — fortschreitenden Zeit t. Die zwischen der Schloßeinheit, vgl. E, und der Schlüsseleinheit, vgl. S, ausgetauschten drei Signale 1, 2 und 3 stellen z. B. codierte Funk-, Licht- oder Ultraschallsignale dar.

Die Erfindung weist also eine tragbare Schlüsseleinheit auf. Diese enthält einen schlüsselseitigen Sender, einen schlüsselseitigen Empfänger und einen schlüsselseitigen Rechner, vgl. S.

Die Erfindung weist außerdem eine am Objekt — hier beispielhaft an dem Kfz — angebrachte Schloßeinheit auf, die einen schloßseitigen Sender, einen schloßseitigen Empfänger, einen schloßseitigen Rechner, vgl. E, sowie eine für sich bekannte Ausgangseinheit zur Steuerung, vgl. V, des Schlosses — z. B. zur Steuerung der Verriegelung des Schlosses — enthält.

Bei der Erfindung stellen die verschiedenen Codes der Signale, vgl. n, x, y und y + 1, jeweils Wechselcodes dar, also keine Codes, die stets gleichbleibend benutzt werden. Die erfindungsgemäß benutzten Codes stellen dabei — gerade wenn die zweite Gruppe von Wechselcodebildung gewählt wurde — sowohl im schlüsselseitigen als auch im schloßseitigen Rechner algorithmisch gebildete Codes aus einer sehr langen Codefolge dar, falls dann die von der Schloßeinheit E und der von der Schlüsseleinheit S benutzten Algorithmen untereinander völlig identisch sind, dann kann man den ersten Code 1 bezeichnen als Code n, wodurch dann aber der zweite Code x als n + 1 bezeichnet werden kann, und in entsprechender Weise der dritte Code y als n + 2, usw.

An sich kann der erste Algorithmus, der zur Bildung des ersten und des dritten Signales 1 und 3 benutzt wird, wie unten beschrieben auch identisch mit dem zweiten Algorithmus sein, der zur Bildung des zweiten Signales 2 benutzt wird. Zuerst sei aber ein Fall beschrieben, bei dem der erste und der zweite Algorithmus verschieden sind.

Um die Codes in den Rechnern S und E gemäß der zweiten Wechselcodebildungsgruppe bilden und um die empfangenen Signale, vgl. 1 bis 3, im empfangenden Rechner auf ihre Gültigkeit prüfen zu können, sind dann, wenn die schlüsselseitigen Signale 1 und 2 nach einem ersten Algorithmus, die schloßseitigen Signale 2 aber nach einem anderen, zweiten Algorithmus gebildet sind, sowohl im schloßseitigen als auch im schlüsselseitigen Speicher jeweils beide Algorithmen gespeichert, also sowohl jener erste Algorithmus, der zur Bildung der Codes des schlüsselseitigen Signale 1 und 3 nötig ist, als auch jener zweite Algorithmus, der zur Bildung der Codes des schloßseitigen Signales 2 nötig ist. Außerdem ist dann in beiden Speichern gespeichert, welcher Code zuletzt als gültige Codes für das Signal 3 und/oder 2 und/oder 1 benutzt wurden; es kann dort in den Speichern — alternativ oder zusätzlich — aber auch jener Code oder jene Codes gespeichert sein, die als nächster aktuell gültiger Code n bzw. x des ersten und des zweiten Signales 1 und 2, evtl. auch als nächster gültiger Code y des dritten Signales zu benutzen ist. Je mehr Codes dann von den zukünftig gültig werdenden Codes im voraus besonders im schloßseitigen Speicher gespeichert sind, um so rascher kann der schloßseitige Rechner auf den Empfang von schlüsselseitigen Signalen 1 und 3 reagieren.

Bei dem hier erläuterten Beispiel der Erfindung werden die einzelnen, jeweils aktuell für die Schlüsseleinheit S gültigen Codes also stets durch die Betätigung der Schlüsseleinheit S gemäß dem ersten Algorithmus fortgeschaltet, wobei aber im Prinzip der "zweite" Algorithmus, der von der Schloßeinheit E zur Ausstrahlung des zweiten Code 2 bzw. x als Antwort auf den empfangenen ersten Code 1 bzw. n benutzt wird, auch anders als der erste Algorithmus aufgebaut sein kann. Der Fachmann kann anhand seines Fachwissens und seiner Fachliteratur unschwer jene Details selbst modifizieren, die zu modifizieren nötig sind, wenn er den Wechselcode gemäß der oben angegebenen ersten Gruppe bildet. Nur um die ohnehin großen sprachlichen Schwierigkeiten bei der Beschreibung der Erfindung nicht zu groß werden zu lassen, wird im Folgenden stets stillschweigend davon ausgegangen, daß beim erläuterten Beispiel der Erfindung der Wechselcode gemäß der zweiten Gruppe gebildet wird.

Bei der Erfindung sendet also der schlüsselseitige Sender bei der Betätigung der Schlüsseleinheit zuerst zum schloßseitigen Empfänger der Schloßeinheit ein gemäß dem ersten Algorithmus gebildetes erstes Signal 1 aus, das mit einem ersten, aktuell gültigen Code n — enthalten in der dem ersten Algorithmus entsprechenden Codefolge — moduliert ist. Wenn der Rechner E der Schloßeinheit den vom schloßseitigen Empfänger empfangenen ersten Code n als den derzeit gültigen ersten Code n des Schlüsselsystemes erkennt, dann sendet danach die Schloßeinheit E ihrerseits als Antwort das gemäß ihrem eigenen, zweiten Algorithmus f(n) gebildete Signal 2, das mit dem zweiten, aktuell gültigen Code x der dem zweiten Algorithmus entsprechenden Codefolge moduliert ist, zum schlüsselseitigen Empfänger S zurück.

Wenn der Rechner S der Schlüsseleinheit den vom schloßseitigen Sender gesendeten Code x als den als Antwort gültigen zweiten Code x des Schlüsselsystemes erkennt, dann sendet die Schlüsseleinheit S ihrerseits wieder als Antwort das dritte Signal 3, das gemäß dem ersten Algorithmus mit dem dritten, dann aktuell gültigen Code y moduliert ist, zum schloßseitigen Empfänger.

Die Schloßeinheit S steuert schließlich mittels ihrer Ausgangseinheit V das Schloß — z. B. die Verriegelung dieses Schlosses — , wenn der schloßseitige Rechner E das dritte Signal 3 mit dem dann gültigen Code y empfing.

Nur wenn alle drei ausgetauschten Signale 1, 2 und 3 entsprechend dem erfindungsgemäßen Verfahren richtig codiert waren, wird das Schließsystem durch die

Fernsteuerung betätigt. Die für Einbrecher sehr große Schwierigkeit, einen solchen kompliziert codierten Dialog nachzubilden, bietet eine sehr große Sicherheit gegen den Einbruch bzw. gegen den Diebstahl des Fahrzeuges.

Sobald der schloßseitige Rechner E den Code des dritten Signales 3 als gültig erkannte — erst dann —, stellt sich der schloßseitige Rechner auf einen neuen aktuell gültigen Code für ein nächstes erstes Signal 1 ein. Dabei kann sich dann dieser schloßseitige Rechner E z. B. auf den unmittelbar nächsten, gemäß dem ersten Algorithmus gebildeten Code y+1 — oder auf einen bestimmten folgenden Code y+k mit einem dem betreffenden Schließsystem vorgegebenem Wert k — als jenen ab jetzt gültigen nächsten Code einstellen, den dieser Rechner für ein nächstes Signal 1 anerkennen würde. Der schlüsselseitige Rechner S stellt sich dann, wenn er das zweite Signal 2 als gültig erkannte und daher das dritte Signal 3 aussenden konnte, ebenfalls auf denselben Code y+I bzw. y+k als den nächsten aktuell gültigen Code für die nächste Betätigung des Schlosses, also für sein nächstes erstes Signal 1 ein.

Um den Einbruch besonders zu erschweren, kann man zwei verschiedene Algorithmen für die Schlüsseleinheit und die Schloßeinheit auswählen.

Dann unterscheidet sich der erste Algorithmus also wirklich vom zweiten Algorithmus. Dann könnte der Einbrecher, auch wenn er ein gemäß dem zweiten Algorithmus gebildetes zweites Signal 2 mitabgehört hätte, besonders schwer erraten, nach welchem ersten Algorithmus das erste und das dritte Signal 1 und 3 gebildet wurde. Diese Schwierigkeit hat der Einbrecher besonders dann, wenn sein mithörendes Aufzeichnungsgerät zusätzlich Schwierigkeiten hatte, die drei verschiedenen Signale 1, 2 und 3 deutlich voneinander zu trennen, — nämlich besonders dann, wenn eine besonders rasche Aufeinanderfolge der drei Signale 1 bis 3 eingerichtet wurde, oder wenn gar das Schließsystem bewußt so dimensioniert wurde, daß sich die drei Signale 1 bis 1 für einem mithörenden Einbrecher kaum entwirrbar zeitlich überlappen.

Überdies schaltet der erfindungsgemäß benutzte Wechselcode nach einer jeden ordnungsgemäßen Betätigung des Schließsystemes auf jeweils neue andere, dann aktuell gültige Codes der Codefolge/Codefolgen um, bevor der Einbrecher unmittelbar die mitgehörten, aufgezeichneten Codes für den Einbruch benutzen kann. Dem Einbrecher ist also nicht nur die Ermittlung des ersten Algorithmusses erschwert.

In diesem zuletzt angegebenen Fall bildet der zweite, in dem schloßseitigen Rechner E benutzte Algorithmus das von der Schloßeinheit abzustrahlende zweite Signal 2 stets aus dem empfangenen ersten, als gültig erkannten Signal n nach einer zweiten, dafür gewählten besonderen Rechenregel, die z. B. unmittelbar den Code n des zuvor empfangenen ersten Signales 1 umwandelt und die sich dann als Funktion f(n) darstellen läßt, so daß dann der auf das zweite Signal 2 modulierte Code x = f(n) ist. Das dritte Signal 3 kann in diesem Falle sogar mit dem — gemäß dem ersten Algorithmus — auf den Code n unmittelbar folgenden Code n+1 moduliert sein, weil der Code x des zweiten Signales 2 nicht gemäß dem ersten Algorithmus gebildet wird.

Im Prinzip kann aber das zweite Signal 2 auch unabhängig vom jeweiligen digitalen Wert des Code n, nämlich gemäß einem zweiten, vom ersten Algorithmus verschiedenen Algorithmus codiert werden, wenn der zweite Algorithmus ebenfalls für sich ein Wechselcode ist, der z. B. ebenfalls ursprünglich mit einem besonderen, für den zweiten Algorithmus bestimmten Urcode initialisiert wurde. Das mit dem Code x gemäß dem zweiten Algorithmus codierte zweite Signal 2 wird dann sofort als Antwort auf das empfangene, als gültig anerkannte Signal 1 abgestrahlt, wobei dann die benutzten Algorithmen für den Einbrecher besonders undurchsichtig sind.

Man kann aber die Erfindung auch so dimensionieren, daß der erste Algorithmus identisch mit dem zweiten Algorithmus ist, so daß der erste Code n, der zweite Code x und der dritte Code y die nach demselben ersten Algorithmus gebildeten, aufeinanderfolgenden Codes n, x=n+1, y=n+2 ein und derselben Codefolge bilden. Damit erreicht man eine besonders unkomplizierte Anordnung bzw. einen besonders unkomplizierten Betrieb des Schließsystemes. Der Benutzer des Fahrzeuges ist auch schon bei dieser Variante der Erfindung sehr stark gegen einen Einbruch durch Codemanipulationen gesichert, und zwar viel stärker, als wenn das Schließsystem ohne Dialog schon nach Aussendung des ersten Signales 1 das Steuersignal der Ausgangseinheit V abgeben würde. Für den Einbrecher ist es ja sehr schwierig, den benutzen ersten Algorithmus ausfindig zu machen, — der Einbrecher müßte nämlich sowohl den ersten Code n als auch den übernächsten Code n+2 der dem ersten Algorithmus entsprechenden Codefolge simulieren können, um im Fahrzeug die Steuerung V des Schlosses auszulösen.

Bei der Erfindung kann übrigens der erste Code n für den schloßseitigen Rechner E in für sich bekannter Weise, vgl. die bereits zitierte

— DE-A1-35 36 378,

in einem Fangbereich F liegen, der durch eine deutlich begrenzte Anzahl von jenen Codes gebildet wird, die der schloßseitige Rechner E gemäß dem ersten Algorithmus als die nächsten gültigen Codes zu erwarten hat. In der Figur wurde angenommen, daß vor (!) der Aussendung des ersten Signales 1 der schloßseitige Rechner E auf einen fangbereich F eingestellt war, der beispielhaft durch die — gemäß dem ersten Algorithmus — aufeinander folgenden Codes n-1, n, n+1 ..... n+m gebildet wurde; in diesem Falle umfaßte also der Fangbereich F insgesamt m+1 aufeinander folgende Codes.

Dann kann zumindest in den meisten Fällen in für sich bekannter Weise automatisch der Verlust der Synchronisation

— jenes Code, der in der Schlüsseleinheit als — gemäß dem ersten Algorithmus — nächster aktuell gültiger Code gespeichert ist,
— mit jenem anderen Code, der zur selben Zeit in dem Speicher der Schloßeinheit als — gemäß dem ersten Algorithmus — nächster zu erwartender aktuell gültiger Code gespeichert ist,

durch eine automatische Nachsynchronisation rückgängig gemacht werden, — falls nämlich der Code in der Schlüsseleinheit durch ein versehentliches mehrmaliges Betätigen dieser Einheit versehentlich um viele Schritte fortgeschaltet wurde, ohne daß auch der Code in der Schloßeinheit fortgeschaltet wurde, vgl. z. B. die bereits erwähnte

— DE-A1-35 36 378.

Nach dem Empfang des dritten Signales 3 — bevorzugt erst dann — richtet sich der schloßseitige Rechner E auf einen z. B. mit dem Code y+1 beginnenden nächsten Fangbereich F ein. Dieser Code y+1 kann z. B. der gemäß dem ersten Algorithmus gebildete Code n+3 sein.

Um eine Nachsynchronisation bei versehentlichen Betätigungen der Schlüsseleinheit zumindest in den meisten Fällen vermeiden zu können, kann aber der Betrieb der Erfindung auch so eingerichtet werden, daß die Schlüsseleinheit S nur dann bei ihrer Betätigung vom ersten gültigen, ausgesendeten Code n auf den gemäß dem ersten Algorithmus gebildeten dritten Code y seiner gemäß dem ersten Algorithmus gebildeten Codefolge fortschaltet, wenn der Empfänger der Schlüsseleinheit wirklich bereits den gültigen zweiten Code x als Antwort — und zwar innerhalb einer kurzen Frist von z. B. wenigen Millisekunden — als Antwort empfing. Andernfalls verbleibt der Rechner S der Schlüsseleinheit beim Code n als den weiterhin immer noch aktuell gültigen Code für die Aussendung eines ersten Signales 1. Eine weitere Verbesserung der Sicherheit gegen Manipulationen durch Einbrecher kann man dadurch erreichen, daß man die Zeit zwischen dem Empfang des zweiten Signales 2 und der Aussendung des dritten Signales stark verkürzt, — z. B. indem nicht mehr der Benutzer des Fahrzeuges eigens einen Druckknopf an der Schloßeinheit zur Aussendung des dritten Signales 3 drücken muß, — sondern indem die Schlüsseleinheit vollautomatisch auf den Empfang des (richtig codierten) zweiten Signales hin sofort das dritte Signal 3 aussendet.

Der Rechner E der Schloßeinheit schaltet in diesem Fall nur dann gemäß dem ersten Algorithmus auf den nächsten Code y+1 als den von ihm für ein nächstes erstes Signal 1 (!) gültigen nächsten Code y+1 der gemäß dem ersten Algorithmus gebildeten Codefolge fort, wenn die Schloßeinheit E das dritte Signal 3 richtig mit dem dafür gültigen Code y innerhalb einer für das dritte Signal 3 dann üblichen, kurzen Frist von z. B. Bruchteilen von Millisekunden empfing.

Für den dann nur noch recht seltenen Fall, daß zwar das erste Signal 1 mit dessen Code, vgl. n, sowie auch das zweite Signal 2 mit dessen Code, vgl. x, einwandfrei übertragen wurde, daß aber das dritte Signal 3 mit dessen Code y — warum auch immer — nicht, oder nicht mit dem unbedingt nötigen Leistungspegel, den schloßseitigen Empfänger erreichte, kann man zur Vermeidung des dann drohenden Synchronisationsverlustes vorsichtshalber im schloßseitigen Rechner E zusätzlich einen, wenn auch nur wenige Fortschaltungen umfassenden Fangbereich F einrichten, der z. B. nur zwei oder drei Fortschaltungen — z. B. n und n+1 und n+2 — des Codes umfaßt. Dann ist auch in diesem recht seltenen Fall — zumindest bis zu einem gewissen Grade — ebenfalls eine automatische Nachsynchronisation in einem sehr kleinen fangbereich F gewährleistet.

Wenn sich, wie bereits oben dargelegt, das erste, das zweite und das dritte Signal (1 bis 3) zweitlich mehr oder weniger, aber nur so stark überlappen, daß die von den Empfängern empfangenen Codes (n, x, y) noch von den zugeordneten Rechnern (S, E) auf ihre Gültigkeit geprüft werden können, ist dem Einbrecher besonders stark erschwert, durch das Mithören eines Dialoges Rückschlüsse auf den benutzten Algorithmus/die benutzten Algorithmen zu ziehen.

Die Erfindung gestattet also, durch einen entsprechenden Betrieb ein Schließsystem zu bieten, das gerade die Vorteile der in den vorhergehenden Verfahrensansprüchen angegebenen Maßnahmen auszunutzen gestattet.

Patentansprüche

1. Verfahren zum Betrieb eines in einem Dialogverfahren durch Signale (1, 2, 3), nämlich codierte Funk-, Licht- oder Ultraschallsignale, fernsteuerbaren — z. B. verriegelbaren und entriegelbaren — Schließsystemes eines Objektes, z. B. eines Kfz,

— mit einer tragbaren Schlüsseleinheit, die einen schlüsselseitigen Sender, einen schlüsselseitigen Empfänger und einen schlüsselseitigen Rechner (S) enthält,

— mit einer am Objekt angebrachten Schloßeinheit, die einen schloßseitigen Sender, einen schloßseitigen Empfänger, einen schloßseitigen Rechner (E) und eine Ausgangseinheit zur Steuerung (V) des Schlosses — z. B. zur Steuerung der Verriegelung des Schlosses — enthält,

— wobei die Codes (n, x, y, y+1) der Signale (1, 2, 3) jeweils Wechselcodes darstellen, die algorithmisch verknüpfte, sowohl im schlüsselseitigen als auch im schloßseitigen Rechner generierte Codefolgen (z. B. Code n, Code x = n+1, Code y = n+2....) darstellen, und

— wobei die einzelnen Codes, die jeweils in der Schlüsseleinheit (S) für deren auszusende Signale (1, 3) gebildet werden, jeweils — z. B. durch die Betätigung der Schlüsseleinheit oder gesteuert von einer Uhr — gemäß einem ersten Algorithmus fortgeschaltet werden,

dadurch gekennzeichnet,

— daß bei Betätigung der Schlüsseleinheit dessen Sender zuerst ein erstes Signal (1) zum schloßseitigen Empfänger sendet, wobei das erste Signal (1) mit einem gemäß dem ersten Algorithmus gebildeten ersten, aktuell gültigen Code (n) aus der dem ersten Algorithmus entsprechenden Codefolge moduliert ist,

— daß danach die das erste Signal (I) empfangende Schloßeinheit, wenn ihr Rechner (E) den empfangenen ersten Code (n) als den gültigen ersten Code (n) erkennt, ihrerseits als Antwort ein zweites Signal (2) zum schlüsselseitigen Empfänger sendet, wobei das zweite Signal (2) mit einem gemäß einem zweiten Algorithmus (f(n)) gebildeten zweiten, aktuell gültigen Code (x=f(n)) aus der dem zweiten Algorithmus (f(n) entsprechenden Codefolge moduliert ist,

— daß danach die Schlüsseleinheit ihrerseits als Antwort, wenn ihr Rechner (S) den mit dem zweiten Signal (2) empfangenen Code (x=f(n)) als gültigen zweiten Code (x) des Schlüsselsystemes erkennt, ein drittes Signal (3) zurück zur Schloßeinheit (E) sendet, wobei das dritte Signal (3) mit einem gemäß dem ersten Algorithmus gebildeten dritten, dafür aktuell gültigen Code (y) aus der dem ersten Algorithmus entsprechenden Codefolge moduliert ist,

— und daß die Schloßeinheit (E) mittels ihrer Ausgangseinheit (V) das Schloß steuert, wenn der schloßseitige Rechner (E) den empfangenen dritten Code (y) als den für das dritte Signal (3) gültigen Code erkennt.

2. Verfahren nach Patentanspruch 1, dadurch gekennzeichnet,

— daß der zweite Algorithmus stets den Code (n) des empfangenen ersten, als gültig erkannten Signals (1) nach einem zweiten Algorithmus (f(n)) umcodiert (x = f(n)), der sich vom ersten Algorithmus unterscheidet, und

— daß der schloßseitige Sender dieses umcodierten Code (x) auf das zweite Signal (2) moduliert zum schlüsselseitigen Empfänger sendet.

3. Verfahren nach Patentanspruch I, dadurch gekennzeichnet,

— daß der erste Algorithmus identisch mit dem zweiten Algorithmus ist, so daß der Code (n) des ersten Signals (1), der Code (x) des zweiten Signals (2) und der Code (y) des dritten Signals (3) jeweils nach demselben Algorithmus gebildete, aufeinanderfolgende Codes (n, x = n + 1, y = n + 2) ein und derselben Codefolge darstellen.

4. Verfahren mit einem durch die Betätigung der Schloßeinheit fortschaltbaren Wechselcode, nach einem der vorhergehenden Patentansprüche, dadurch gekennzeichnet,

— daß der Code (n) des ersten Signals (1) für den schloßseitigen Rechner (E) in einem fangbereich (f) liegen muß, der durch eine deutlich begrenzte Anzahl von jenen Codes (n-1, n, n+1, ... , n+m) gebildet wird, die der schloßseitige Rechner (E) gemäß dem ersten Algorithmus als die nächsten gültigen Codes zu erwarten hat.

5. Verfahren mit einem durch die Betätigung der Schloßeinheit fortschaltbaren Wechselcode, nach einem der Patentansprüche 1 bis 3, dadurch gekennzeichnet,

— daß der Rechner (S) der Schlüsseleinheit nur dann bei deren Betätigung vom ersten gültigen, ausgesendeten Code (n) auf den mit dem dritten Signal (3) auszustrahlenden, gemäß dem ersten Algorithmus gebildeten Code (y = n + 1, oder y = n + 2) der gemäß dem ersten Algorithmus gebildeten Codefolge fortschaltet, wenn die Schlüsseleinheit (S) das zweite Signal (2) richtig mit dem dafür gültigen Code (x) innerhalb einer für das zweite Signal (2) üblichen, kurzen Frist (z. B. Bruchteile von Sekunden) empfing.

6. Verfahren nach Patentanspruch 5, dadurch gekennzeichnet,

— daß der Rechner (E) der Schloßeinheit nur dann gemäß dem ersten Algorithmus auf den nächsten Code als den von ihm für ein erstes Signal (!) gültigen Code (y + 1) der gemäß dem ersten Algorithmus gebildeten Codefolge fortschaltet, wenn die Schloßeinheit (E) das dritte Signal (3) richtig mit dem dafür gültigen Code (y) innerhalb einer für das dritte Signal (3) üblichen, kurzen Frist (z. B. Bruchteile von Millisekunden) empfing.

7. Verfahren nach Patentanspruch 5 oder 6, dadurch gekennzeichnet,

— daß in der Schloßeinheit (E) trotzdem ein wenn auch nur wenige Fortschaltungen umfassender Fangbereich (F) eingerichtet ist.

8. Verfahren nach einem der vorhergehenden Patentansprüche, dadurch gekennzeichnet,

— daß sich das erste, das zweite und das dritte Signal (1 bis 3) zweitlich mehr oder weniger,

aber nur so stark überlappen, daß die von den Empfängern empfangenen Codes (n, x, y) noch von den zugeordneten Rechnern (S, E) auf ihre Gültigkeit geprüft werden können.

9. Schließsystem zur Durchführung des Verfahrens nach einem der vorhergehenden Patentansprüche.

Hierzu 1 Seite(n) Zeichnungen

– Leerseite –

Int. Cl.[5]: E 05 B 49/00
Veröffentlichungstag: 3. Februar 1994